مديرية البحث العلمي في وزارة التعليم العالي في سوريا

ندوة

التقانات الحديثة للمعلومات و الاتصالات و دورها في التعليم بمختلف مراحله

محور

الذكاء الاصطناعي وأمن المعلومات

عنوان البحث :

الأمن في التعليم عن بعد
Distance Learning Security

د.عمَّار ريماوي

الأمن في التعليم عن بعد

ملخص البحث :

بعد انتشار التعليم عن بعد بشكل واسع ظهرت مشكلات عديدة رافقت هذا النوع من التعليم مثل المشكلات التقنية والمشكلات البرمجية ومشكلات الكوادر التعليمية والمشكلات الأمنية وتم التركيز في هذا البحث على المشكلات الأمنية واقتراح مناسب لتجاوز بعض المشكلات باستخدام تقنية الجلسات Sessions المطورة وتأمين المحتوى العلمي من الاختراقات.

Distance Learning Security

Abstract:

When distance learning had become widespread, many problems came out. I.e. technical problems, software problems, learning staff problems and learning security problems. In this paper we have concentrate on security problems and suggest a suitable solution to protect website and its learning contents using a developed session.

مقدمة:

كان للتطور الهائل الذي طرأ على الاتصالات والانترنت دوراً كبيراً في انتشار التعليم عن بعد لما له من مزايا حيث أنه غير مرتبط بالزمان والمكان، ويمكن من الحصول على تجربة تعليمية متناسبة مع كافة الأشخاص حيث تؤمن لكل شخص اختيار الدراسة المتوافقة والمتناسبة مع خياراته وحاجاته وإمكانياته، وإمكانية تبادل الآراء والحوار والنقاش مع أعداد كبيرة جدا من الدارسين مما يساعد على التشارك بالمعلومات وتبادل الآراء، واستخدام العديد من أدوات الإيضاح والوسائل التعليمية السمعية والبصرية والتي قد لا تتوافق دائما في حالات التعليم التقليدي، وإمكانية التقييم الفوري والسريع للمتعلم مما يساعده على التعرف على نتائجه وتصحيح أخطائه بالإضافة إلى توفير التعليم في المناطق النائية...

وبما أن الاعتماد الرئيسي للتعليم عن بعد على مواقع شبكة الانترنت فقد بدأت مشكلات الانترنت تنتقل إلى هذا التعليم وأهم هذه المشكلات هي المشكلات الأمنية لما تؤثر بشكل كبير على هذا النوع من التعليم، فمصداقية هذا التعليم وموثوقيته تعتمدان على ندرة الاختراقات الحاصلة من هذا النوع وخاصةً في مجال تأمين المحتوى العلمي والمحاضرات المباشرة والامتحانات المباشرة وكذلك على التقني في الزمن الحقيقي.

المشكلات التي تواجه التعليم عن بعد:

المشكلات التقنية Technical Problems

- البنية التحتية ومشاكل الاتصال.

يعتمد التعليم عن بعد على توفر بنية تحتية من النوع الجيد تتيح عمليات الاتصال عالي الجودة المطلوب في التعليم عن بعد كونه يعتمد في جزء منه على المحاضرات المباشرة والامتحانات ... وغالباً لا تتوفر هذه البنية في المناطق النائية التي تحتاج هذا النوع من التعليم أكثر من غيرها.

- الحاجة إلى تحديث التجهيزات بشكل مستمر.

توجد ضرورة ملحة تستلزم مواكبة التجهيزات المستخدمة للتطور السريع في تقنيات التعليم عن بعد وطرائق توفير الأمن اللازم.

- **مشكلة البرمجيات Software Problems**

- عدم توافقية بين الأنظمة والبرمجيات الضعيفة التي لا تخدم بالشكل المطلوب.

يستخدم العاملون في هذا المجال (المدرسين والطلاب) أنظمة وبرمجيات متعددة قد لا تكون متوافقة بالضرورة . على سبيل المثال قد لايستطيع الطالب متابعة الدرس بسبب عدم التوافق في لغة الواجهات...

- عدم اعتماد معيار موحد لصياغة المحتوى التعليمي.

لم يعتمد حتى الآن معيار موحد لصياغة المحتوى التعليمي . وتعدّد أنماط استعراض وصياغة المحتوى التعليمي يسبب بعض الاربكات ... البعض يعتمد برنامج AuthorWare والآخر يستخدم برنامج MacromediaFlash والآخر يستخدم Acrobat ، رغم وجود بعض المعايير العالمية مثل Scorm ، LMS ...

- **مشكلات الكوادر التعليمية Learning Staff Problems**
  - عدم التأهيل الكافي للمدرسين والطلاب.

يؤدي ذلك إلى عدم تمكن المدرس من ايصال المادة التعليمية بالرغم من كفاءته العلمية وكذلك عدم تمكن الطالب من الاستفادة من المادة التعليمية بالرغم من نباهته.

  - ضعف مشاركة التربويين الاختصاصيين في هذا النمط من التعليم.

يحتاج المحتوى التعليمي إلى تربويين اختصاصين قادرين على صياغته بالطريقة المناسبة والتي تمكن من ايصاله إلى الطالب بالشكل الذي يمكنه من استيعاب هذا المحتوى على النحو الأكمل.

- **مشكلات أمن التعليم Learning Security Problems**
  - استحالة تحقيق الأمن المطلق.

عندما ترسل الأرقام الثنائية للمعالج لا يفرق بين 1 الأولى و1 الأخيرة مثلاً، فهما متماثلان، ولا يمكن تميزهم بسبب عدم وجود كتابة يدوية تحليليةِ أَو بصماتِ أَو شهادةِ الأصالةِ.

ويتم الاختراق، إذا يَستبدلُ المهاجمَ أحد تلك الأرقام 1 بشكل سري مَع الـ0 ، وتكون البرامج العادية للمعالجة ليست ذات سلطةُ لمعرفة أن هذا الـ0 ليس حقيقيا فهو يَبْدو مثل أيّ 0آخر، وماعدا ذلك يَكُونَ الـ1 أيضاً مثله مثل أي 1 آخر.

إن البرامج الجيدة (التي تأخذ هذه القضية بالحسبان) والتي كتبت مِن قِبل المبرمجين المحترفين هي التي تميز ذلك، حيث تقوم هذه البرامج بمقارنة الموقع الآخر في الذاكرة، ومعرفة أن هذه الأرقام عدلت أم لا.

فإذا طُبّقتْ هذه المراقبةِ بشكل سيئ، أَو لم تنفذ نهائياً، تكون عملية الاختراق قد تمت بدون أن تكتشف، وبالتالي فإن تطبيقات التعليم عن بعد والتي تعمل مباشرة على الشبكة تزيد من الشكوك حول إمكانية الاختراقات، وذلك لأن مصدر إدخال المعلومات في الشبكة يمكن أن يكون غير موثوق. وهذا يعود لسبب جوهري وهو أن مُدخل هذه المعلومات غير معروف، إضافة إلى الحصانة (الشكلية) التي يتمتع بها مهاجمو الشبكة، على الأقل ريثما يتم تعقب أثرهم من خلال عناوين أجهزتهم IP Address والتي يمكن تغيرها بسهولة.

وبالتالي فإن الاختراقات التي تهدد التطبيقات التي تعمل على الشبكة عديدة ولا يمكن تعقبها لدرجة أن أصبح من الروتين بالنسبة للخبراء التحدث عن تدارك الخطر الذي يسببه الاختراق

عوضاً عن القضاء عليه. وأصبح هذا أمراً طبيعياً وهذا يسبب أزمة كبيرة في حالة الحاجة الماسة إلى وجود الحماية المطلقة كما في مواقع التجارة الالكترونية والبنوك والتعليم الالكتروني.

- توقف الخدمة Denial of Service (DOS):

يوجد العديد من أنواع الهجوم DOS نذكر أهمها:

- **استهلاك عرض الحزمة :**

حيث يقوم المهاجم باستهلاك كامل عرض الحزمة في نظام شبكة الضحية وذلك باغراق شبكة الضحية بكمية هائلة من الطلبات مثل ...GET, SYN : وغيرها، مما يؤدي إلى استهلاك كامل لعرض الحزمة وإيقاف الموقع المستهدف أو النظام المهاجم تماماً عن العمل، ويكون ذلك إما بالهجوم مباشرة Direct Attack حيث ينتصر في هذه الحالة من لديه عرض حزمة أكبر (مثلاً 56 Kbps في مواجهة 128 Kbps)، أو القيام بربط العديد من المواقع من أجل إغراق نظام الضحية حيث يقوم المهاجم باستخدام أنظمة البث broadcast في شبكات أخرى من أجل تضخيم الهجوم، ويستفيد في هذه الحالة من عرض حزمة تلك الشبكة .

- **استهلاك الموارد:**

هذا النوع من الهجوم يعتمد على استهلاك الموارد في نظام الضحية عوضا عن استهلاك عرض الحزمة. أهم الموارد التي يتم استهدافها هي : CPU, Memory, Kernel, File system ... وغيرها، ويؤدي انخفاض الموارد في النظام إلى عدم استقراره وانهياره في نهاية الأمر .

- **الثغرات البرمجية في مكونات النظام :**

لا يوجد نظام أو برنامج خالٍ تماماً من الثغرات مهما بلغت دقة تصميمه، يوجد عدة طرق لاستغلال هذه الثغرات مثلا بارسال Packets غير متوافقة مع المعايير القياسية لـ بروتركول TCP/IP المحددة من قبل RFC إلى نظام الضحية مما يؤدي إلى نتائج تختلف حسب نوع البرنامج من توقف الخدمة، أو توقف النظام، أو ضياع المعلومات، أو فيضان المكدس stack وغير ذلك .

كما يوجد أنواع أخرى من هجمات DOS إلا أنها أقل فعالية وغير مستخدمة على نطاق واسع، وقد يحصل ذلك دون قصد في حال الطلبات البسيطة لصفحة الدراسة من خلال المتصفح فإذا تم تكرارها بشكل كبير من المرات قد يجبر المخدم الخاص بموقع الدراسة على زيادة كميات النقل وفي الحالات الشديدة لمثل هذه الطلبات تتحمل دورات المعالج ونطاقات

البث أكثر من طاقتها بكثير وبالتالي تتعثر وتتوقف النشاطات الشرعية القائمة تماماً، مما يؤدي إلى تعطل الدراسة.

- تأثيرات Griefers , Trools , Pranksters على التعليم عن بعد.

بالرغم من أن هؤلاء قد لا يبدون خطرين مقارنة مع الهاكرز Hackers واللصوص Hijackers في الشبكة ، فإن طبقة المستخدمين المعروفة بالـ Griefers , Trools Pranksters هم الأكثر إزعاجاً بنسبة عشرات الأضعاف، ويستطيعون القضاء على المتعة في المجتمع الافتراضي (عملية الدراسة عن بعد) بشكل مباشر وفوري ولابد من توضيح المفاهيم التالية:

الـGriefers: هم المستخدمين الذين يستمتعون بإيذاء الآخرين ومهاجمتهم. فعندما تلاحظ وجود بعض المستخدمين المجهولين في أي محاضرة مباشرة على الشبكة Online والذين يختبئون تحت اسم مجهول Screen Name يكونون الـGriefers حيث يقومون بإزعاج شديد ومؤذٍ جداً حيث يقومون بإرسال التعليقات تقوم بإزعاج كل من المدرسين والطلاب.

الـTrools: يستمتعون بكونهم مهاجمين وأيضاً فإنهم يقومون بسرقة اسمك أثناء التعليقات في المنتديات العلمية الموضوعة من قبل المدرسين ويقومون بالإجابة عنك على أسئلة موجهة إليك مما يجعل إجاباتك غير صحيحة وقد تعرضك للعلامات السيئة أو للمسائلة القانونية.

الـPranksters: فيقومون بإدخال تعليمات بلغات مثل Html أو Javascript إلى مايسمى Plain Text، وذلك بغية تشويه مظهر صفحة الانترنت، أو قد يتظاهرون بأنهم أشخاص آخرين، أو قد يأتون بطرق عديدة يعملون بها لإلهاء الآخرين عما كان من المفروض أن يكون عملاً مهماً. كأن يطرحوا مواضيع لا تمت بصلة إلى العملية التدريسية وهذا لإلهاء أفراده عن الأفكار التي من المفروض أن يركزوا عليها.

- تأثير الافتراءات وسوء التخزين.

الافتراء Defamation: هو استخدام المحترفين للتطبيقات الخاصة بك لإيذاء الآخرين سواء على مستوى الأشخاص أو المؤسسات عن طريق الدمى المتحركة sock puppets (وهي إجراءات تستخدم غالباً في عمليات التصويت)، إن عملية التعليق Posting الذي يقوم بها شخص غير معروف Anonymous غالباً هو أمر اعتيادي لا مشكلة فيه، وغموض هذه التعليقات Posts يقلل من احتمالية كونها قابلة للتصديق، وعلى كل حال هي قابلة للإزالة عندما يتم اكتشافها. ولكن المشكلة هي حصول عملية Posting باسمك وتحوي الكثير من المواضيع الغير صحيحة والمفترية، وهنا حتى لو استطعت إزالتها إثر ملاحظتك لها، قد تعرضك للمحاكمة والمسؤولية، على الأقل من قبل المؤسسة التعليمية التابع لها، على الرغم من إنك لست من قام بتعليق الرسالة.

سوء التخزين Abuse of Storage: قد تتيح المواقع التعليمية أماكن خاصة للتخزين مقدمة للطلاب لخدمة المحتوى التعليمي (كأن تسمح لهم باستخدام مساحات مجانية لتخزين مواقع إنترنت تجريبية) ومواقع كهذه تجذب العديد من هؤلاء المزعجين الذين يرغبون بتخزين الوثائق الغير شرعية والمثيرة للفوضى وليس الملفات الخاصة بالعمليات التعليمية، كما يستخدمون المساحات المجانية التي توفرها هذه المواقع عوضاً عن الدفع من أجل الحصول عليها.

- تأثيرات Malware (الفيروسات Viruses والديدان Worms و برمجيات التجسس Spyware وحصان طروادة Trojans).

إحدى أشهر الهجومات والاختراقات الموجهة أوتوماتيكيا على الإطلاق، وبالتأكيد أسوأها وأكثرها ضرراً، فالدودة Worm أو الفيروس Virus هو برنامج صغير يقوم بتنزيل نفسه على جهاز الكمبيوتر الخاص بك دون معرفتك وفي أغلب الأحيان من خلال ملحقات الرسائل الالكترونية Attachments أو من خلال تحميلها بطريقة ضمنية عند تحميل Download التطبيقات أو البرامج، وهناك فرق تقني بسيط بين الاثنين : فالدودة قابلة للوجود من تلقاء نفسها بينما يحتاج الفيروس إلى أن يتخفى وراء إحدى التطبيقات أو المستندات، ويعمل من خلالها، والهدف الرئيسي للفيروس أو الدودة هو أن يعمل على نسخ نفسه ويتضاعف محاولاً الانتقال إلى أجهزة أخرى والانتشار، والهدف الثانوي هو نشر الفوضى على جهاز المضيف، من خلال حذف وتعديل الملفات، وفتح الباب لتدفق الـSpams والملفات والرسائل غير المرغوبة إلى جهاز المضيف، أو الرسائل المنبثقة Popping up من مختلف الأنواع، مما يجعل الجهاز المصاب (جهاز الأستاذ مثلاً) عرضة لإرسال هذه الفيروسات أو الديدان إلى أجهزة أخرى (أجهزة الطلاب مثلاً).

أما Spyware فهي البرمجيات التي تتجسس على الأجهزة وترسل معلومات عنها لتسهل عمليات الاختراق فيما بعد و Trojans برامج خبيثة تختفي وراء برمجة أو بيانات غير مؤذية بحيث تتمكن من السيطرة ومن ثم تعمل أشكالها المختارة للضرر، مثل تخريب ملفات الإقلاع على قرصك الصلب. وأخيراً جميع الـMalware تجعل من الجهاز المصاب مركزاً لإنتشارها.

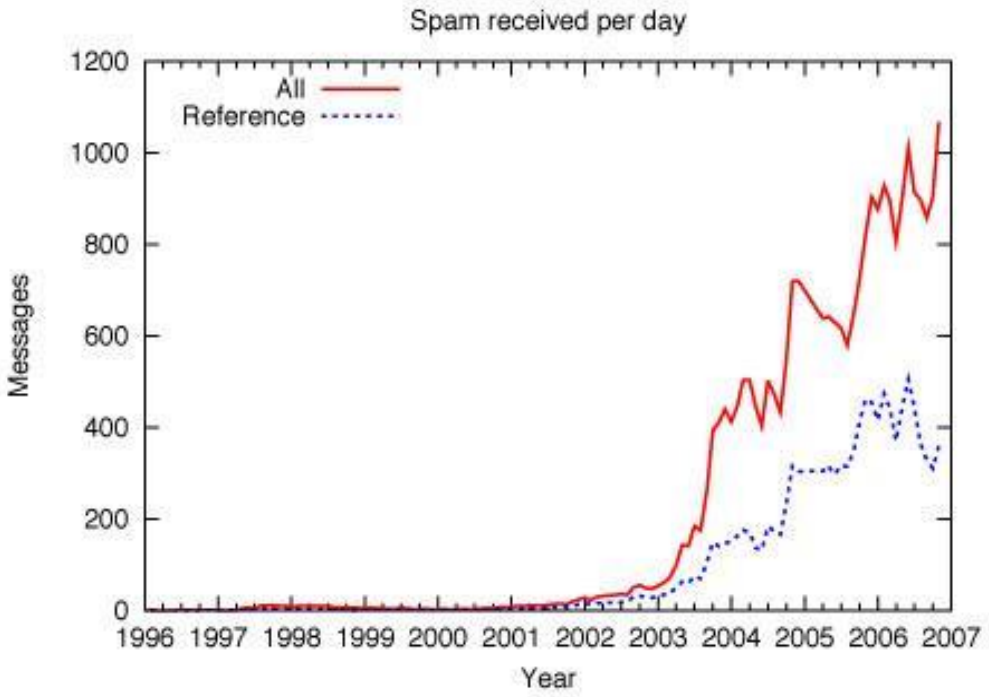
تأثير السبامات Spams في أمن التعليم.

الـSpam: هو إرسال الرسائل الغير مجدية بكميات كبيرة وغالباً تكون غير مرحب بها، هذا النوع من الهجوم هو هجوم أوتوماتيكي من نمط مختلف، لأنها تبدو لمتلقيها رسائل عادية وإن كانت كثيرة، وقد لا يستغرق من المستخدمين وقتاً طويلاً ليبدءوا بالتعرف على هذه الرسائل أو أغلبها على الأقل، ولكن تستغرق المخدمات Servers والتي تتحمل عبء نقل هذه الرسائل وقتاً أطول للتعرف عليها، ولكن الـSpams تجعل كل من المخدم والمستخدم

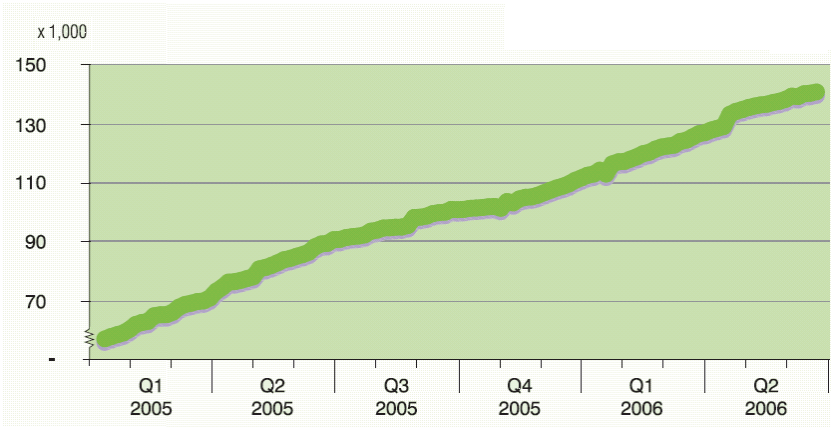
يعاني من الخدمات الغير مرحب بها، وقد يؤدي التصفح غير المقصود لها لإعادة إرسالها ثانية ومن خلال عنوانك الالكتروني مما يجعلها أمنة للطرف الآخر (من مدرس إلى طلابه) وهي محملة بالفيروسات.

فتخيل أن تأتيك رسالة من مدرسك أو العكس وتتحدث عن التسويق لمواقع تجارية وهمية.

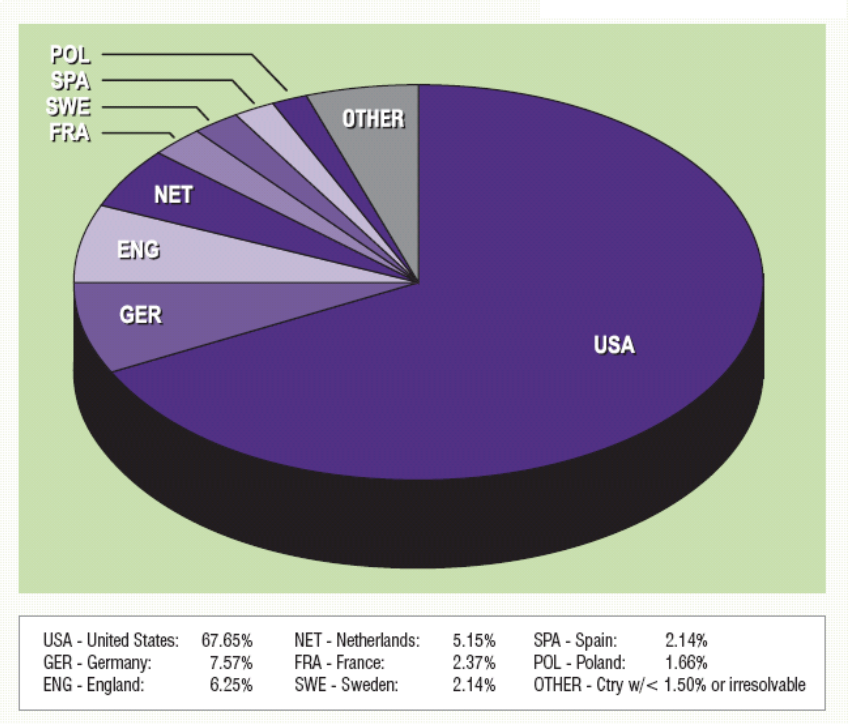
بعض الإحصائيات والمخططات التي تبين تزايد عمليات الاختراق:



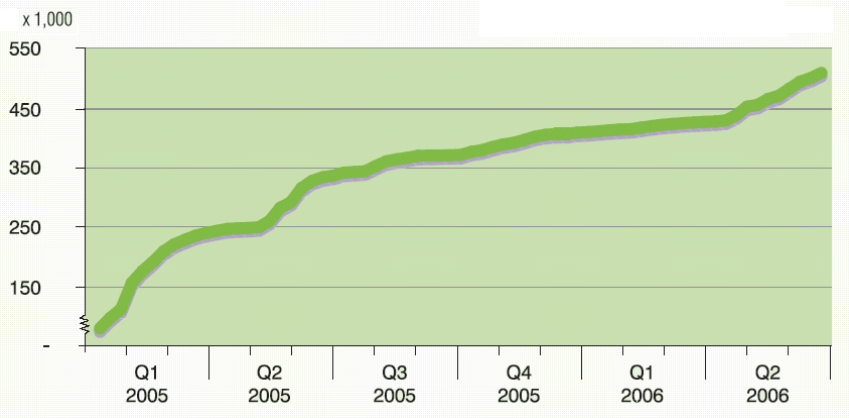
كمية السبامات Spams الواصلة لمستخدم واحد يومياً ولمعدل شهر من 1996 وحتى 2007 ومن خلال عناوين إيميلات متعددة.



تزايد عدد برامج الـ Spyware



الدول المستضيفة لـ Spyware

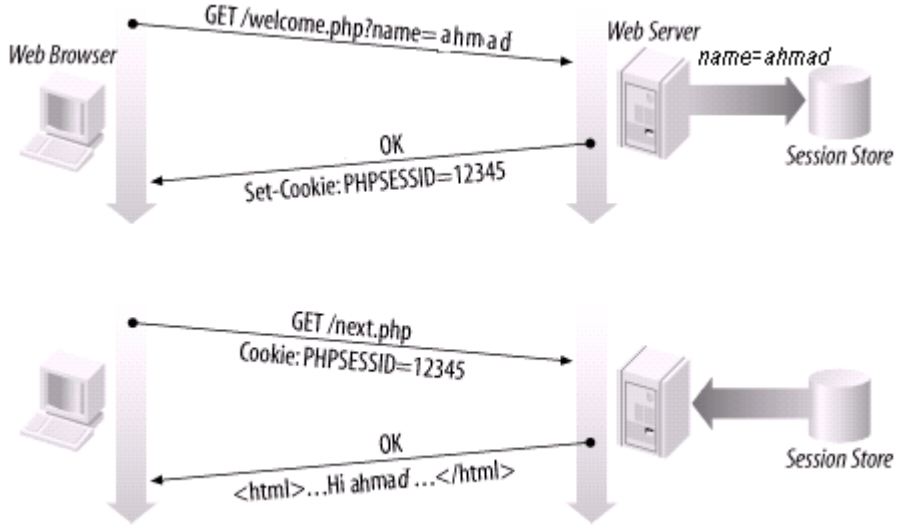


تزايد عدد مواقع الـ Malware

تقنية الجلسات Sessions:

عند الانتقال من صفحة الى أخرى في موقع معين فإن بروتوكول الـ HTTP لا يمكنه معرفة أن تلك الصفحات قد تم تصفحها من قبل نفس الشخص، ولذلك وببساطة فإن الـ Session هي

ملف على المخدم يمكن من خلاله تخزين قيمة معينة للرجوع اليها في حال قام نفس الشخص بالانتقال من صفحة الى أخرى من خلال الـ cookies المزروع في جهاز ذلك الشخص.
إذاً التعرف على الشخص الذي يقوم بتصفح الموقع هو الهدف الرئيسي للـ Session.



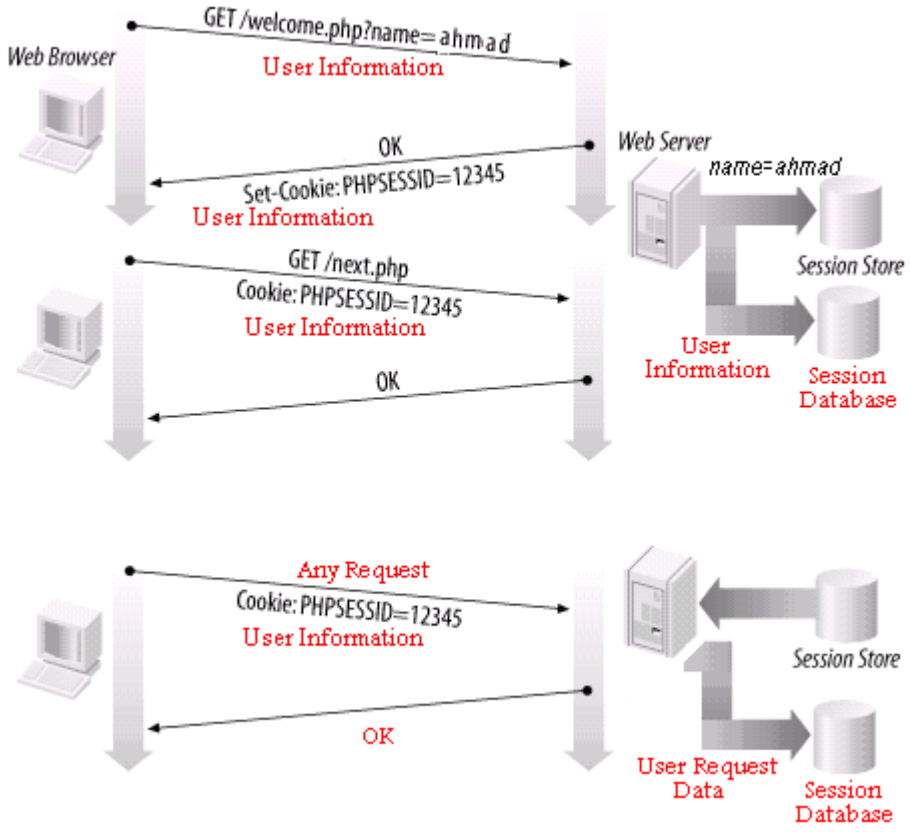
مخطط يوصف طريق عمل الجلسة العادية

تطوير تقنية الجلسات Sessions لرفع مستوى أمن المواقع التعليمية:

تمكن هذه التقنية مدير الموقع التعليمي من ضبط أمنه بمراقبة المستخدمين عند قيامهم بالدخول إلى المحتوى التعليمي أو تعديله أو إدخال أي نوع من البيانات إليه ، وكشف أي تلاعب يمكن أن يحدث خلال ذلك.

فبعد التحقق من اسم المستخدم وكلمة المرور يقوم الموقع بانشاء جلسة عادية في مخزن الجلسات على المخدم تحتوي على بيانات تتوافق مع البيانات الموجودة في الكوكيز التي قام الموقع بزرعها في جهاز المستخدم. وفي كل طلب يتم مطابقة بيانات الجلسة الموجودة على المخدم مع بيانات الكوكيز الموجودة على جهاز المستخدم لتحقيق هذا الطلب له.

وفي الجلسة المطورة يقوم الموقع بالإضافة إلى عمل الجلسة العادية بتخزين معلومات إضافية عن جهاز المستخدم أثناء زرع الكوكيز . وعند أية طلبية يقوم الموقع بالتحقق من معلومات الجهاز ومحتويات الكوكيز وعندما تتم المطابقة يتم تحقيق الطلبية وتسجيل نسخة عن الطلب في قاعدة بيانات مخصصة بذلك ، كما هو مبين في الشكل التالي:

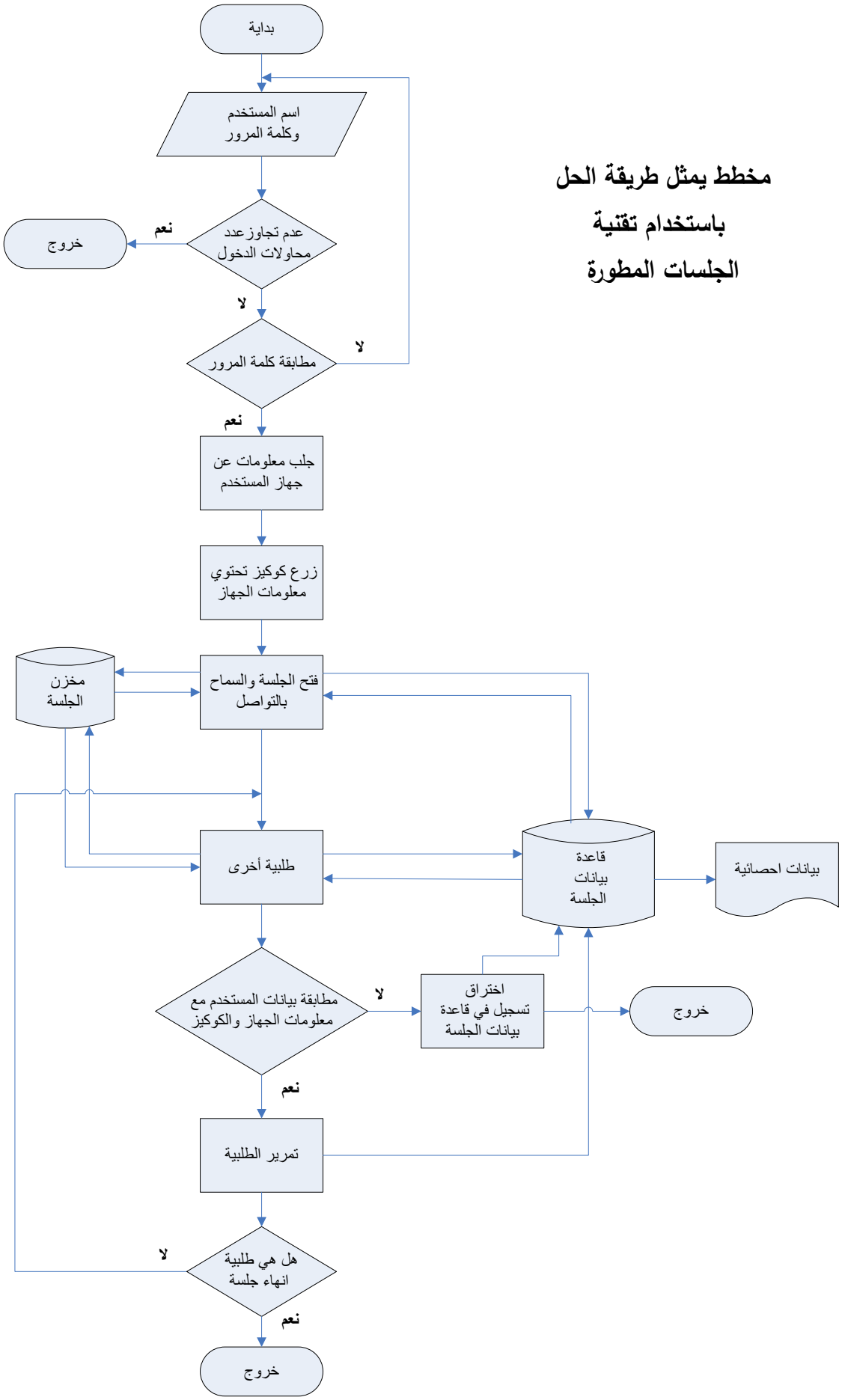


مخطط يوصف طريق عمل الجلسة المطورة

وهذا يتيح لمدير الموقع مايلي :

- حماية الموقع من الـ Griefers , Trools , Pranksters.
- حماية الموقع من الـ Malware.
- تأمين المحتوى العلمي من الاختراقات.
- تسجيل جميع تحركات المستخدم على هذا الموقع.
- إمكانية القيام بإحصائيات متنوعة.

مخطط يمثل طريقة الحل
باستخدام تقنية
الجلسات المطورة



الجزء البرمجي الخاص بتخزين الجلسة في قواعد البيانات:

```
/* بداية الجلسة */
session_start();

 class session
{
   /*اسم الجدول الخاص بالتخزين */
   var $ses_table = "sessions";
   /* متحول التأكد من الاتصال بقواعد البيانات */
   var $db_con = "Y";


   /* متحولات التصال بقواعد البيانات */
   var $db_host = "localhost";
   var $db_user = "root";
   var $db_pass = "root";
   var $db_dbase = "education";


   /* إنشاء الاتصال بقواعد البيانات */
   function db_connect() {
      $mysql_connect = @mysql_pconnect ($this->db_host,
                                 $this->db_user,
                                 $this->db_pass);
      $mysql_db = @mysql_select_db ($this->db_dbase);


      if ($db_con) {
         return FALSE;
      } else {
         return TRUE;
      }
   }


   /*فتح قاعدة البيانات وبدأ وضع البيانات */
   function _open($path, $name) {
      if ($this->db_con == "Y") {
         $this->db_connect();
      }
```

```
    return TRUE;
}

/* إغلاق الجلسة */
function _close() {
    $this->_gc(0);
    return TRUE;
}

/* قراءة البيانات من قواعد البيانات */
function _read($ses_id) {
    $session_sql = "SELECT * FROM " . $this->ses_table
                . " WHERE ses_id = '$ses_id'";
    $session_res = @mysql_query($session_sql);
    if (!$session_res) {
        return '';
    }

    $session_num = @mysql_num_rows ($session_res);
    if ($session_num > 0) {
        $session_row = mysql_fetch_assoc ($session_res);
        $ses_data = $session_row["SES_VALUE"];
        return $ses_data;
    } else {
        return '';
    }
}

/* كتابة بيانات جديدة في القاعدة */
function _write($ses_id, $data) {
    $session_sql = "UPDATE " . $this->ses_table
                . " SET ses_time='" . time()
                . "', ses_date='" .date('d/m/Y')
                . "', ses_value='$data' WHERE ses_id='$ses_id'";
    $session_res = @mysql_query ($session_sql);
    if (!$session_res) {
        return FALSE;
    }
    if (mysql_affected_rows ()) {
        return TRUE;
```

```
        }
        $session_sql = "INSERT INTO " . $this->ses_table
                . " (ses_id, ses_time, ses_start, ses_date, ses_value)"
                . " VALUES ('$ses_id', '" . time()
                . "', '" . time() . "','" .date('d/m/Y'). "', '$data')";
        $session_res = @mysql_query ($session_sql);
        if (!$session_res) {
           return FALSE;
        }       else {
           return TRUE;
        }
    }
    /* حذف بيانات الجلسة */
    function _destroy($ses_id) {
        $session_sql = "DELETE FROM " . $this->ses_table
                . " WHERE ses_id = '$ses_id'";
        $session_res = @mysql_query ($session_sql);
        if (!$session_res) {
           return FALSE;
        }       else {
           return TRUE;
        }
    }


    /* حذف بيانات الجلسة التراكمية */
    function _gc($life) {
        $ses_life = strtotime("-5 minutes");


        $session_sql = "DELETE FROM " . $this->ses_table
                . " WHERE ses_time < $ses_life";
        $session_res = @mysql_query ($session_sql);



        if (!$session_res) {
           return FALSE;
        }       else {
           return TRUE;
        }
    }
}
```

خاتمة:

لقد قمنا بدراسة عدد واسع من التهديدات الأمنية التي قد يواجهها أي تعليم يعمل عن طريق الشبكة ونحن هنا لا نثير المخاوف حيث أن كل هذه المشاكل يتم مواجهتها بطريقة أو بأخرى ومع اختلاف وتنوع المستويات من قبل كل التطبيقات المستخدمة على شبكتنا اليوم .

وبالرغم من أننا قد لا نستطيع وبصورة مطلقة حماية أنفسنا ضد هجوم أو اختراق عالي الفعالية ولكن يمكننا أن نفعل الكثير كمبرمجين لنجعل الهجومات الناجحة أمراً نادر الحدوث.

المراجع

1- Pro PHP Security - Chris Snyder and Michael Southwell.
2- PHP Security Guide - http://phpsec.org/.
3- Notes on PHP Session Security - Harry Fuecks - www.sitepoint.com.
4- A Hacker's Guide to Protecting Your Internet Site and Network - http://newdata.box.sk/bx/hacker/copy.htm.
5- PROFESSIONAL PHP Programming, Jesus Castangnetto and Harish Rawat, Wrox.
6- MySQL/PHP Database Applications, Jay Greenspan and Brad Bulger, M&T Books.
7- MySQL Reference Manual, MySQL AB.
8- Web Database Applications with PHP, and MySQL - Hugh E. Williams, David Lane.
9- The practical solution of requirements using PHP - http://www.wellho.net/.
10- Web Based Session Management - TechnicalInfo.
11- www.webroot.com.
12- http://www.spamnation.info/stats/.